

Appl. No. 09/390,362
Amdt. Dated: 09/30/2004
Reply to Office Action of: 08/28/2003

REMARKS

Applicant wishes to thank the Examiner for reviewing the present application.

No amendments have been effected to the specification or the claims. The replacement sheet containing Figure 3 includes amendments correcting various typographical errors. Accordingly, no new subject matter has been added to the application.

The present invention relates to a method of digitally signing a message exchanged between a pair of correspondents. The correspondents share a public key and the signer has a private key from which the public key is derived. The method divides a message to be sent between the correspondents and hides one portion of the message while leaving the other portion "in the clear" to increase bandwidth efficiency. The following operations then occur:

- (a) utilize one portion to compute a first signature component;
- (b) use the first signature component and the other portion to form an intermediate signature component;
- (c) use the intermediate component and the private key to provide a second signature component; and
- (d) combine the first component, second component, and the other portion to provide a signature.

The step (d) constitutes the output of the system. It shall be noted that the output constitutes a combination of the first and second components and the other portion of the message. The "other portion" is consequently also signed but sent "in the clear" as it is used as an input to the verification process. Please see page 4, lines 9-12 of the specification which exemplifies this.

A method for verifying a message which has been subdivided into a pair of portions (bit strings) from a signature of a purported signer is also provided to recover the message originally subdivided and signed.

Appl. No. 09/390,362
Amdt. Dated: 09/30/2004
Reply to Office Action of: 08/28/2003

The Examiner has rejected Claim 1 under 35 U.S.C. 103(a) as being unpatentable over European Patent Application No. EP 0918274 A2 to McCollom (hereafter "McCollom") in view of U.S. Patent No. 5,915,024 to Kitaori et al. (hereinafter "Kitaori").

Applicant respectfully submits that McCollom does not describe a method reading on claim 1, but provides a method with an output which is in fact distinctly different from that provided by the steps recited in claim 1. The missing elements from McCollom are likewise not found in Kitaori and as such, the combination of McCollom in view of Kitaori lacks all of the elements of claim 1 and would not generate a similar output.

McCollom summarizes his method for securing data using signatures in column 4, between lines 34 and 56 and referring to Figure 1. The method receives a data signal which has one or more data components. The data components are typically one or more elements of the signal and therefore McCollom does not intentionally subdivide the signal, but merely breaks the signal into its inherent components. In step 104, a signature is generated on one or more of the data components. This signature is then combined with one or more of the actual components to create a combined signal (step 106). The combined signal is then encrypted in step 108 and a second signature is generated to produce an encrypted signal signature in step 110.

As stated in column 4, lines 54-56, the output is the encrypted signal signature. This is built from a combination of the first signature and actual data which was encrypted and signed. Referring back to column 4, line 5-12, McCollom states that the result is a digital signature of the encrypted combination, which is a further indication that the output is a signature on the encrypted signal. In the Examiner's analysis, he has equated step (d) to what has been described by McCollom in Col. 3, lines 11-20. It is clearly stated in this passage from McCollom that the second signature is applied to the encrypted combined signal which is an encrypted version of the first signature component combined with another data component.

McCollom does not therefore perform the step of combining a first signature component,

Appl. No. 09/390,362
Amdt. Dated: 09/30/2004
Reply to Office Action of: 08/28/2003

second signature component, and an original portion of data to provide a signature used for transmission (i.e. step (d)). In fact the second signature in McCollom is derived from an encrypted version of a combination of the first signature and a data component. As a result, the output of McCollom differs from that resulting from the steps of claim 1.

A second embodiment described by McCollom similarly only outputs a lone fingerprint (used synonymously with "signature" by McCollom) and not a signature which is a combination of a first signature component, a second signature component and a portion of the original message as recited in step (d) of claim 1.

The Examiner has combined the teachings of Kitaori and McCollom to allege an obvious equivalent to the present invention. McCollom when reviewed separately lacks the final step recited in claim 1 (i.e. step (d)) as well as the use of a private and public key pair. It would therefore be required that Kitaori would have to at least clearly teach the missing elements which are lacking in McCollom to provide the motivation to arrive at the present invention. Applicant respectfully submits that Kitaori, although making reference to private and public key pairs, teaches a system which applies signatures to multiple segments of a document and in no instance does Kitaori describe step (d) recited above. It is therefore believed that a combination of Kitaori and McCollom does not read on claim 1 since the final step of the present invention does not appear in either document and, in fact each reference generates an output which differs from that produced by the steps recited in claim 1.

The objective of a cryptographic system is to produce an output which can be transmitted between correspondents in a secure manner. Since the output generated according to the present invention differs significantly from the output generated by McCollom, particularly with regards to the final step, the manner in which this objective is attained of each of these systems must be different. McCollom lacks any teaching of the final step recited in claim 1, in fact he explicitly states that the final output is the encrypted signal signature. Kitaori teaches a system using a private and public key pair, however also fails to describe the missing step not found in McCollom required to equate McCollom with what has been recited in claim 1. As such, a

Appl. No. 09/390,362
Amdt. Dated: 09/30/2004
Reply to Office Action of: 08/28/2003

combination of Kitaori and McCollom would not result in the present invention and claim 1 would not be obvious from such a combination since that combination does not provide the method recited in claim 1.

Accordingly it is submitted that claim 1 clearly distinguishes over the combination suggested by the Examiner and is in condition for allowance. Claims 2 to 6 are either directly or indirectly dependent upon claim 1 and are therefore believed to distinguish over the prior art cited by the Examiner.

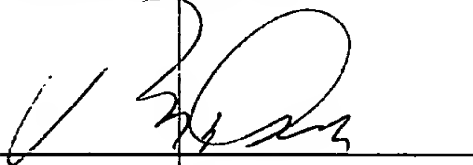
The Examiner has also rejected claim 7 as being unpatentable over McCollom in view of Kitaori. It is believed that the Examiner has improperly equated the verification method recited in claim 7 with a step found in McCollom in which a signal is received. The verification method of claim 7 involves verifying a message which has been sub-divided and signed (e.g. according to the method of claim 1). The Examiner refers to Col. 3, lines 11-20 and Col. 7, lines 30-40. These citations taken from McCollom describe the method outlined above in which the signal is to be signed and not how a signed message is to be verified. It is believed that the Examiner has been mistaken in what occurs when the apparatus in McCollom "receives" a signal. This does not equate to receiving a signed message to be verified, in fact the apparatus is actually referring to the original signal which is to have an encrypted signal signature generated for it. McCollom does not teach a verification method as claim 7 recites, however an apparatus for generating an encrypted signal signature.

It is also believed that the teachings of Kitaori do not describe what McCollom fails to provide in describing a method for verifying a sub-divided message. Kitaori does teach the use of a public and private key pair, however cannot be viewed as teaching what has been described by the present invention when it is combined with McCollom. Accordingly it is submitted that claim 7 clearly distinguishes over the combination suggested by the Examiner and is in condition for allowance. Claims 8 to 13 are either directly or indirectly dependent upon claim 7 and are therefore believed to distinguish over the prior art cited by the Examiner.

Appl. No. 09/390,362
Amdt. Dated: 09/30/2004
Reply to Office Action of: 08/28/2003

Applicant requests early reconsideration and allowance of the present application.

Respectfully submitted,



Ralph A. Dowell
Agent for Applicant
Registration No. 26,868

Date: September 30, 2004

Dowell & Dowell, P.C.
Suite 406
2111 Eisenhower Avenue
Alexandria, VA 22314
USA

Tel: (703) 415-2555

JRO/BSL/jsm